# Research on Computer Network Information Security and Its Protection Countermeasures

# Shao Ju, Tan Zhong\*

Hubei Three Gorges Polytechnic, Yichang, Hubei, China

Keywords: Computer, network information security, protection countermeasures

Abstract: With the continuous development and improvement of China's scientific and technological level and information technology, computer technology plays a more and more important role in people's daily life. However, with the increasing amount of data in the computer network, many computer network security problems emerge, which hinder the smooth operation of the computer network. Therefore, this paper first analyzes the key factors affecting computer network information security, and then puts forward specific network information security protection strategies for reference.

## **1. Introduction**

With the continuous development of modern society, computer network information has gradually become an important part of social production and life, and its security has also been highly concerned by social groups. Once the computer network system is at risk or attacked by virus, it is very easy to damage the network database and even cause unpredictable economic losses to users. In this case, it is very necessary to strengthen the discussion of computer network information security.

## 2. Overview of Computer Network Security

Computer network plays an important role in the political, economic and cultural fields. China is a large country in computer production and use. According to the data of market research structure, the number of network users in China has continued to grow in recent years and has exceeded 1 billion by 2021 (see Figure 1). Computer network information security is facing severe pressure and challenges. Computer network information security involves many fields. In the economic field, the combination of computer network and operators can effectively save the cost of human resources, provide convenient information security support for enterprise operators, and ensure the orderly management of network production and operation. In the political field, strengthening the security of computer network information can ensure that state secrets are not stolen, and ensure the smooth development of national political construction and infrastructure construction. In the field of culture, computer network information security has a direct impact on cultural resource sharing and cultural exchange. Therefore, strengthening computer network information security can enhance the diversity of social culture. In recent years, China has also established a computer network information security mechanism and started the research on computer network information security and protection technology. In addition, China has also invested a lot of human and material resources in computer hardware, network system software and data maintenance, and achieved corresponding results. These practices have improved the information security coefficient of computer network and strengthened the ability of information security protection. However, China's computer network information security protection system is not perfect, and the factors affecting computer network information security still exist. Therefore, China should strengthen computer security management and protection technology, create a good social environment and promote the continuous progress of social economy.



Figure 1 Scale of Internet users in China from 2018 to 2021.

## 3. Key Factors Affecting Computer Network Information Security

## 3.1. Virus invasion

In the current development of computer network technology, there are many factors affecting network information security, one of which is virus intrusion. Virus is a major aspect of computer security that spreads through the Internet in the current development of computer network, and its harm is huge. If a computer is infected with a computer virus, it will not only cause certain harm to the computer, making the computer appear virus software, reduced fluency, slow response and other phenomena, but also spread to other computers through the computer. At present, network resources are very rich, so computer hackers usually hide computer viruses in the resources that people are interested in. If people click on the resources, their computers will be invaded by viruses. If the computer invaded by the virus is the computer of enterprises and other units, the virus will spread rapidly through the internal network of the enterprise, resulting in the paralysis of the whole computer network chain of the enterprise, which is easy to cause the leakage of core information and secrets within the enterprise, and the negative impact is difficult to predict.

## 3.2. Man-made Network Security Threat

For the current computer network information security, man-made network security threat is also a main factor affecting its security. The most fundamental purpose of computer network security is to protect the user's personal information from infringement. The threat to the computer also comes from the threat to the information stored by others. At present, most of the threats to computer network security are caused by human factors, some of which are unintentional, and some are deliberately caused by hackers. Generally speaking, man-made network security threats mainly include passive and active ways. Among them, the passive mode is often very secret, which is generally difficult to find when using the computer, and this passive attack mode is implicit and will not affect the normal use of the computer, but will intercept and modify the computer information, so the consequences are difficult to predict. The way of active attack is carried out by hackers through certain technical means in order to achieve their own purpose. Hackers often attack selectively in the process of active attack to obtain the information resources they need. This way will destroy the stability of computer use and destroy the computer network.

#### 3.3. Vulnerabilities in the Computer

In addition to the above two points, the vulnerability of the computer itself is also a major factor affecting network information security. The vulnerability of the computer itself mainly refers to the potential security problems existing in the computer, which is mainly caused by the non-standard installation of computer software. At present, various computer application software emerge in endlessly. These software meet the market demand through their own innovation. At the same time, these computer software must have some problems in software development and use. Computer hackers use these loopholes in the use of computers to invade people's computers and make computers infected with viruses. In addition, the internal application program of computer network is also a key factor causing computer to be invaded by virus. When programmers design the internal application program of computer network, if some design rules are found by hackers, there will be a risk of computer intrusion. Therefore, software companies must test the newly developed software in advance and constantly repair the vulnerabilities, so as to better ensure the security of the software.

# 4. Countermeasures of Computer Network Information Security Protection

# 4.1. Strengthening Network Security Awareness

In the process of the continuous application and popularization of economic network, people should have enough security awareness in the application of computer network, pay more attention to information security, and focus on it from the ideological level, so as to reflect the due information security in the process of practice. For example, when people use the computer network for mobile banking login or Alipay account login, some information may be attacked by criminals to steal relevant accounts and passwords, resulting in serious security risks to the user's account information, and even serious economic losses to the user. In this case, we need to attach great importance to security protection, have security awareness, further effectively improve the security level of account passwords, set corresponding security plug-ins, and set different passwords for different accounts. Only when users fundamentally improve their security awareness and have the due risk identification ability, can they improve the network information security of the computer system to a greater extent, improve the security and confidentiality of the whole system, effectively avoid or reduce the invasion of wooden horses and the spread of viruses, ensure that the network system will not be attacked by criminals, and the relevant data information can also be protected.

# 4.2. Installing Firewall and Anti-virus Software

The firewall technology of computer can evaluate the security risk in the process of computer operation, and then monitor the data inside the computer in real time by means of isolation and protection, so as to ensure the long-term normal operation of the computer. By installing a firewall, the computer can find viruses and abnormalities inside the computer in time. Use the advantages and characteristics of firewall to block and process viruses, so as to ensure the security and stability of computer internal data information. In addition to the method of installing firewall inside the computer, computer users can also improve the protection ability of the computer through anti-virus software. Common anti-virus software include Baidu anti-virus, Tencent computer housekeeper, 360 security guard and Kaspersky. Although these anti-virus software have different names, they have significant effects in computer virus processing. Through the installation of anti-virus software, the internal files of the computer can be scanned regularly, which has a good effect of checking and killing viruses. The combination of firewall and anti-virus software can greatly improve the protection ability of computer information and reduce the leakage of data information.

## 4.3. Using File Encryption

By encrypting the important files inside the computer, we can ensure the security and stability of computer data information and improve the protection ability of computer data information. In the daily use of computers, internal files are often transmitted to other computers by means of data transmission. In the process of data transmission, computer users can adopt the way of line encryption to ensure the stability of file transmission and avoid data leakage in the process of transmission. As a common file encryption method in recent years, digital signature plays a good role in the protection of computer data information. The working principle of digital signature is to form two complementary operations through the technical application in the field of public key encryption, so as to avoid the leakage and loss of files in the transmission process and ensure the integrity and non repudiation of files.

#### 4.4. Adhering to the Maintenance and Management of Software and Hardware

Regular maintenance and management of computer software and hardware can enhance the information protection ability of computer. The maintenance and management of computer hardware mainly includes the detection and maintenance of computer equipment. After long-term use of computer equipment, it will cause damage to hardware facilities and affect the normal use of computer equipment. Through regular maintenance, we can find the hardware problems of the computer in time, deal with them by corresponding means and methods, prolong the service life of the computer equipment, and better protect the information security inside the computer. In addition, through the establishment of strict rules and regulations, non staff can be prohibited from entering the computer room to avoid the leakage of computer information. The closed management of the external equipment from stealing data information. The maintenance and management of computer equipment software is mainly carried out by updating the safety protection system. In this way, the vulnerabilities in the computer system can be found in time, the vulnerabilities can be filled by means of system patches, and the probability of virus intrusion can be reduced.

## 4.5. Network Monitoring and Intrusion Detection

With the popularization and popularization of artificial intelligence and big data technology, it provides great convenience for network monitoring and intrusion detection technology. Big data technology has strong data collection and analysis ability, and can collect and sort out various data in the process of computer operation. Then use the principles and characteristics of statistics to analyze the internal data of the computer, so as to judge whether the computer is in a safe state. The combination of artificial intelligence and big data technology can monitor all data in the computer in real time, ensure the stable operation of the computer and prevent the intrusion of viruses and network hackers. Once abnormal changes are found in the internal data of the computer, the network monitoring and intrusion detection system can send a warning to the computer user in time. And make use of the advantages of artificial intelligence and big data to check the abnormally changed data, so as to realize the tracking effect of network virus. When using the method of data tracking to find an exception in a file, it will use the way of clearing the file or formatting to guide the computer user to operate. This series of processes can not only make the computer data information play a good protective role, but also clear the abnormalities inside the computer as soon as possible, so that the computer can return to the normal state as soon as possible.

# 5. Conclusion

The continuous development of computer and Internet technology has brought great convenience to people's daily work and life, but it also brings great hidden dangers. Therefore, in daily work and life, people must improve their understanding of network information security and protection, strengthen the maintenance of hardware and software systems, constantly improve the awareness of information security, and form the habit of setting passwords for important documents. Only when we do these in our daily work can people do a good job in computer network information security and protection.

# References

[1] Fadhil Saif Aamer,Kadhim Lubna Emad,Abdurazaq Sayl Gani. Protection measurements of computer network information security for big data[J]. Journal of Discrete Mathematical Sciences and Cryptography,2021,24(7).

[2] Liu Saie. Computer Network Information Security and Protection Measures under the Background of Big Data[J]. Journal of Physics: Conference Series, 2021, 1881(3).

[3] Yanmei Yang. Computer Network Information Security and Protection Strategy[J]. Frontiers in Economics and Management,2020,1(12).